

Алферов А. П., Зубов А. Ю., Кузьмин А.С. , Черемушкин А. В.

Основы криптографии: Учебное пособие. 3-е изд., испр. и доп. — М.: Гелиос АРВ, 2005. — 480 с, ил.

Написано ведущими специалистами в области криптографии, имеющими многолетний опыт разработки криптографических средств защиты и преподавания дисциплин криптографического цикла в ведущих вузах страны.

Излагаются основные понятия и разделы, позволяющие получить представление о задачах и проблемах современной криптографии. В пособие вошли как традиционные вопросы классификации и оценки надежности шифров, так и системные вопросы использования криптографических методов защиты информации.

Для студентов, аспирантов, изучающих дисциплины по криптографии и компьютерной безопасности, преподавателей, а также широкого круга специалистов, задачами которых являются квалифицированный выбор и организация использования криптографических средств защиты информации.

ОГЛАВЛЕНИЕ

Предисловие от издательства к третьему изданию.....	3
Введение	5
Обозначения	7
Глава 1. Исторический очерк развития криптографии.....	8
Глава 2. Основные понятия	54
§ 2.1. Криптография	54
Конфиденциальность.....	56
Целостность.....	62
Аутентификация	63
Цифровая подпись	65
§ 2.2. Управление секретными ключами	68
Предварительное распределение ключей.....	68
Пересылка ключей	69
Открытое распределение ключей	70
Схема разделения секрета.....	71
§ 2.3. Инфраструктура открытых ключей... ..	72
Сертификаты.....	72
Центры сертификации.....	73
§ 2.4. Формальные модели шифров.....	74
§ 2.5. Модели открытых текстов.....	79
Математические модели открытого текста.....	80
Критерии распознавания открытого текста.....	83
Глава 3. Классификация шифров по различным признакам.....	86
§ 3.1. Математическая модель шифра замены.....	87
§ 3.2. Классификация шифров замены	89
Глава 4. Шифры перестановки.....	95
§ 4.1. Маршрутные перестановки	95
§ 4.2. Элементы криптоанализа шифров перестановки.....	98

Глава 5. Шифры замены	101
§ 5.1. Поточные шифры простой замены.....	101
§ 5.2. Криптоанализ поточного шифра простой замены.....	105
§ 5.3. Блочные шифры простой замены	113
§ 5.4. Многоалфавитные шифры замены.....	121
§ 5.5. Дисковые многоалфавитные шифры замены.....	122
Глава 6. Шифры гаммирования	126
§ 6.1. Табличное гаммирование	126
§ 6.2. О возможности восстановления вероятностей знаков гаммы.....	129
§ 6.3. Восстановление текстов, зашифрованных неравновероятной гаммой.....	132
§ 6.4. Повторное использование гаммы	139
§ 6.5. Криптоанализ шифра Виженера	143
§ 6.6. Ошибки шифровальщика	152
Глава 7. Надежность шифров.....	156
§ 7.1. Энтропия и избыточность языка.....	156
§ 7.2. Расстояние единственности	162
§ 7.3. Стойкость шифров	169
Теоретическая стойкость шифров.....	172
Практическая стойкость шифров.....	179
§ 7.4. Вопросы имитостойкости шифров ...	182
§ 7.5. Шифры, не распространяющие искажений.....	194
Шифры, не распространяющие искажений типа "замена знаков"	195
Шифры, не распространяющие искажений типа "пропуск-вставка знаков"	201
Глава 8. Блочные системы шифрования	205
§ 8.1. Принципы построения блочных шифров.....	206
§ 8.2. Примеры блочных шифров	209

Американский стандарт шифрования данных DES.....	209
Стандарт шифрования данных ГОСТ 28147-89.....	220
§ 8.3. Режимы использования блочных шифров.....	223
§ 8.4. Комбинирование алгоритмов блочного шифрования.....	230
§ 8.5. Методы анализа алгоритмов блочного шифрования.....	231
§ 8.6. Рекомендации по использованию алгоритмов блочного шифрования.....	237
Глава 9. Поточные системы шифрования.....	240
§ 9.1. Синхронизация поточных шифрсистем.....	240
§ 9.2. Принципы построения поточных шифрсистем.....	242
§ 9.3. Примеры поточных шифрсистем	247
Шифрсистема A5	247
Шифрсистема Гиффорда	250
§ 9.4. Линейные регистры сдвига	251
§ 9.5. Алгоритм Берлекемпа — Месси.....	261
§ 9.6. Усложнение линейных рекуррентных последовательностей.....	265
Фильтрующие генераторы.....	265
Комбинирующие генераторы	272
Композиции линейных регистров сдвига.....	274
Схемы с динамическим изменением закона рекурсии	275
Схемы с элементами памяти.....	279
§ 9.7. Методы анализа поточных шифров.....	283
Глава 10. Шифрование в аналоговой телефонии.....	287
§ 10.1. Особенности речевых сигналов	287
§ 10.2. Скремблирование .:	290
§ 10.3. Частотные преобразования сигнала	291
§ 10.4. Временные преобразования сигнала.....	298
§ 10.5. Стойкость систем временных перестановок.....	305
§ 10.6. Системы цифровой телефонии.....	307

Глава 11. Системы шифрования с открытыми ключами.....	310
§ 11.1. Шифрсистема RSA	311
§ 11.2. Шифрсистема Эль-Гамала	318
§ 11.3. Шифрсистема Мак-Элиса	321
§ 11.4. Шифрсистемы на основе "проблемы рюкзака"	323
Глава 12. Идентификация.....	327
§ 12.1. Фиксированные пароли (слабая идентификация).....	328
Правила составления паролей	329
Усложнение процедуры проверки паролей.....	330
"Подсоленные" пароли	330
Парольные фразы.....	331
§ 12.2. Атаки на фиксированные пароли	331
Повторное использование паролей.....	331
Тотальный перебор паролей	332
Атаки с помощью словаря	332
Личные идентификационные номера.....	333
Одноразовые пароли.....	334
§ 12.3. "Запрос-ответ" (сильная идентификация).....	335
"Запрос-ответ" с использованием симметричных алгоритмов шифрования	337
"Запрос-ответ" с использованием асимметричных алгоритмов шифрования	339
§ 12.4. Протоколы с нулевым разглашением.....	341
§ 12.5. Атаки на протоколы идентификации.....	344
Глава 13. Криптографические хэш-функции.....	347
§ 13.1. Функции хэширования и целостность данных.....	347
§ 13.2. Ключевые функции хэширования	350
§ 13.3. Бесключевые функции хэширования.....	354
§ 13.4. Целостность данных и аутентификация сообщений.....	359
§ 13.5. Возможные атаки на функции хэширования.....	362

Глава 14. Цифровые подписи	365
§ 14.1. Общие положения	365
§ 14.2. Цифровые подписи на основе шифрсистем с открытыми ключами.....	369
§ 14.3. Цифровая подпись Фиата-Шамира.....	371
§ 14.4. Цифровая подпись Эль-Гамала.....	372
§ 14.5. Одноразовые цифровые подписи	375
Глава 15. Протоколы распределения ключей	378
§ 15.1. Передача ключей с использованием симметричного шифрования.....	378
Двусторонние протоколы.....	378
Трехсторонние протоколы	381
§ 15.2. Передача ключей с использованием асимметричного шифрования	385
Протоколы без использования цифровой подписи.....	385
Протоколы с использованием цифровой подписи.....	386
Сертификаты открытых ключей	386
§ 15.3. Открытое распределение ключей	387
§ 15.4. Предварительное распределение ключей.....	390
Схемы предварительного распределения ключей в сети связи.....	391
Схемы разделения секрета	398
§ 15.5. Способы установления ключей для конференц-связи.....	401
§ 15.6. Возможные атаки на протоколы распределения ключей.....	404
Глава 16. Управление ключами	408
§ 16.1. Жизненный цикл ключей.....	411
§ 16.1. Услуги, предоставляемые доверенной третьей стороной.....	414
Установка временных меток.....	415

Нотаризация цифровых подписей ..	416
Глава 17. Некоторые практические аспекты использования	
шифрсистем.....	418
§ 17.1. Анализ потока сообщений	418
§ 17.2. Ошибки операторов	419
§ 17.3. Физические и организационные меры при	
использовании шифрсистем	420
Глава 18. Квантово-криптографический протокол открытого	
распределения ключей	423
Квантовый канал и его свойства	423
Протокол открытого распределения ключей	425
Приложение 1. Открытые сообщения и их характеристики	429
Приложение 2. Пример	450
Приложение 3. Элементы алгебры и теории чисел	460
Литература	469